技術情報：Si-R/Si-R brinシリーズ設定例
(「NET-G」とのVPN(IPsec)接続-IPv4_NATトラバーサルあり)

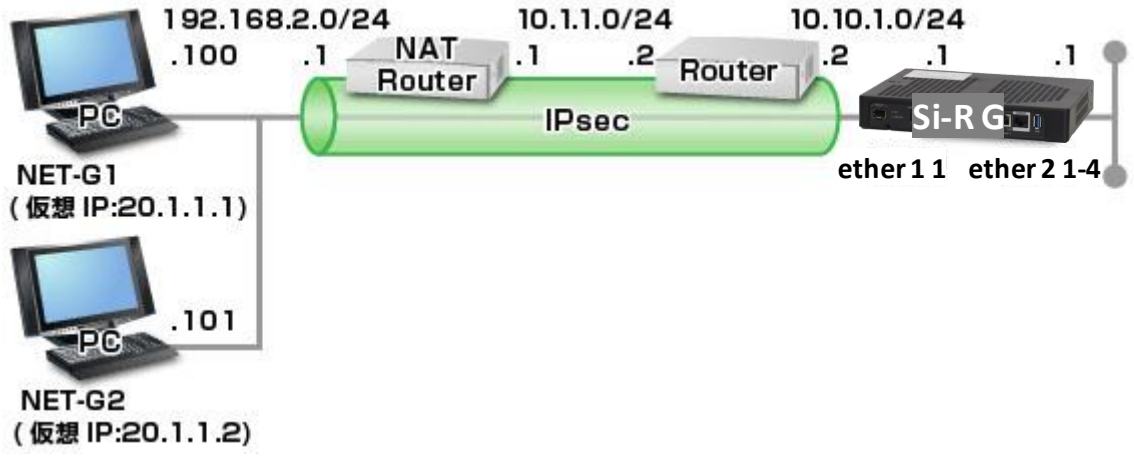
dit_NET-GとIPv4でVPN接続する場合の設定事例です。
NATトラバーサル機能を利用する場合の設定事例です。
NAT RouterではIPsecパススルー機能をoffにして下さい。

[対象機種と版数]
Si-R Gシリーズ V4.06以降

[設定内容]
・Si-R Gのether１1をWAN側、ether２1-4をLAN側とします。
・NET-G側のルータでNAT機能を有効にします。
・LAN側に192.168.1.254/24、192.168.2.254/24を割り当てます。
・IKE/IPsecのパラメータを以下のように設定します。

IKE関連パラメータ	
キー交換モード	アグレッシブモード
暗号化アルゴリズム	AES-256
整合性アルゴリズム	SHA2
DHグループ	1,536bit
事前共有鍵文字列	“sir2-key”,”sir3-key”
装置識別情報	“sir2”,”sir3”
キーの有効時間	480分

IPsec関連パラメータ	
プロトコル	ESP
暗号化アルゴリズム	AES-256
整合性アルゴリズム	SHA2
DHグループ	1,536bit
キーの有効時間	60分/100,000Kbyte



[設定例]
・sir2-keyにはIPsec鍵を設定してください。

Si-R G設定例

```
ether 1 1 vlan untag 1001
ether 2 1-4 vlan untag 1002
lan 0 ip address 10.10.1.1/24 3
lan 0 ip route 0 default 10.10.1.2 1 1
lan 0 vlan 1001
lan 1 ip address 192.168.1.1/24 3
lan 1 vlan 1002
template 0 name NET-G
template 0 interface pool 1 50
template 0 aaa 0
template 0 datalink type ipsec
template 0 ipsec ike protocol esp
template 0 ipsec ike encrypt aes-cbc-256
template 0 ipsec ike auth hmac-sha256
template 0 ipsec ike pfs modp1536
template 0 ike mode aggressive
template 0 ike proposal 0 encrypt aes-cbc-256
template 0 ike proposal 0 hash hmac-sha256
template 0 ike proposal 0 pfs modp1536
template 0 ike nat-traversal use on
template 0 tunnel local 10.10.1.1
aaa 0 name sir
aaa 0 user 0 id sir2
aaa 0 user 0 password sir2
aaa 0 user 0 ip route 0 20.1.1.1/32 1 1
aaa 0 user 0 ipsec ike range any4 20.1.1.1/32
aaa 0 user 0 ike shared key text sir2-key
aaa 0 user 1 id sir3
aaa 0 user 1 password sir3
aaa 0 user 1 ip route 0 20.1.1.2/32 1 1
aaa 0 user 1 ipsec ike range any4 20.1.1.2/32
aaa 0 user 1 ike shared key text sir3-key
syslog pri error,warn,info
syslog facility 23
time zone 0900
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal charset SJIS
```

解説
Si-R_G設定解説

Si-R G

ether 1 1 vlan untag 1001
ether1 1ポートをTag なしVLAN1001に設定します。

ether 2 1-4 vlan untag 1002
ether2 1-4ポートをTag なしVLAN1002に設定します。

lan 0 ip address 10.10.1.1/24 3
LAN0側IPアドレスを設定します。
・10.10.1.1/24：IPアドレス/マスクです。
・3：ブロードキャストアドレスのタイプです。通常は3で構いません。

lan 0 ip route 0 default 10.10.1.2 1 1
スタティックルートを設定します。
・default：デフォルトルートです。
・10.10.1.2：ネクストホップです。
・1：metric値です。通常はこのままで構いません。
・1：distance値です。通常はこのままで構いません。

lan 0 vlan 1001
VLAN ID とlan 定義番号の関連付けを行います。

lan 1 ip address 192.168.1.1/24 3
LAN1側IPアドレスを設定します。
・192.168.1.1/24：IPアドレス/マスクです。
・3：ブロードキャストアドレスのタイプです。通常は3で構いません。

lan 1 vlan 1002
VLAN ID とlan 定義番号の関連付けを行います。

template 0 name NET-G
インターフェースの名前(任意)を設定します

template 0 interface pool 1 50
テンプレート着信で使用するrmt インタフェースの設定をします。
・1：テンプレート着信で使用する開始rmt インタフェース番号です。
・50：テンプレート着信で使用するrmt インタフェース数です。 ◦ 上記設定の場合、rmt1～rmt50の最大50拠点分のtemplate着信が可能です。

template 0 aaa 0
テンプレート着信で認証および着信を行う場合に参照するAAA のグループID を設定します。

template 0 datalink type ipsec
パケット転送方法としてIPsecを設定します。

template 0 ipsec ike protocol esp
自動鍵交換用IPsec情報のセキュリティプロトコルにESP（暗号）を設定します。

template 0 ipsec ike encrypt aes-cbc-256
自動鍵交換用IPsec情報の暗号情報にAES256ビットを設定します。

template 0 ipsec ike auth hmac-sha256
自動鍵交換用IPsec情報の認証情報にSHA256を設定します。

template 0 ipsec ike pfs modp1536
自動鍵交換用IPsec情報のDH(Diffie-Hellman) グループにmodp1536を設定します。

template 0 ike mode aggressive
IKE 情報の交換モードとしてAggressive Mode を設定します。

template 0 ike proposal 0 encrypt aes-cbc-256
IKEセッション用暗号情報の暗号アルゴリズムにAES256ビットを設定します。

template 0 ike proposal 0 hash hmac-sha256
IKE セッション用認証(ハッシュ) 情報にSHA256を設定します。

template 0 ike proposal 0 pfs modp1536
IKE セッション用DH(Diffie-Hellman) グループにmodp1536を設定します。

template 0 ike nat-traversal use on
NATトラバーサル機能を有効にします。

template 0 tunnel local 10.10.1.1
IPsecトンネルの送信元アドレスの設定をします。

aaa 0 name sir
AAA認証のグループ名を設定します。

aaa 0 user 0 id sir2
AAA認証に使用する、認証情報(ユーザID) を設定します。

aaa 0 user 0 password sir2
AAA認証に使用する、認証情報(認証パスワード) を設定します。
・IPsecのAggressive Modeを利用する場合は、相手装置識別情報を設定します。
・ユーザID と認証パスワードは同じ値を設定してください。

aaa 0 user 0 ip route 0 20.1.1.1/32 1 1
スタティックルートを設定します。
・20.1.1.1/32：宛先ネットワーク/マスクです。
・1：metric値です。通常は1で構いません。
・1：distance値です。通常は1で構いません。

aaa 0 user 0 ipsec ike range any4 20.1.1.1/32
自動鍵交換用IPsec 情報の対象範囲を設定します。
・any4：IPsec 対象となる送信元IP アドレス/マスクです。
・20.1.1.1/32：IPsec 対象となる宛先IP アドレス/マスクです。

aaa 0 user 0 ike shared key text sir2-key
IKEセッション確立時の共有鍵（Pre-shared key）を設定します。

aaa 0 user 1 id sir3
AAA認証に使用する、認証情報(ユーザID) を設定します。

aaa 0 user 1 password sir3
AAA認証に使用する、認証情報(認証パスワード) を設定します。
・IPsecのAggressive Modeを利用する場合は、相手装置識別情報を設定します。
・ユーザID と認証パスワードは同じ値を設定してください。

aaa 0 user 1 ip route 0 20.1.1.2/32 1 1
スタティックルートを設定します。
・20.1.1.2/32：宛先ネットワーク/マスクです。
・1：metric値です。通常は1で構いません。
・1：distance値です。通常は1で構いません。

aaa 0 user 1 ipsec ike range any4 20.1.1.2/32
自動鍵交換用IPsec 情報の対象範囲を設定します。
・any4：IPsec 対象となる送信元IP アドレス/マスクです。
・20.1.1.2/32：IPsec 対象となる宛先IP アドレス/マスクです。

aaa 0 user 1 ike shared key text sir3-key
IKEセッション確立時の共有鍵（Pre-shared key）を設定します。

syslog pri error,warn,info
syslog facility 23
システムログ情報の出力情報／出力対象ファシリティの設定をします。通常はこのままで構いません。

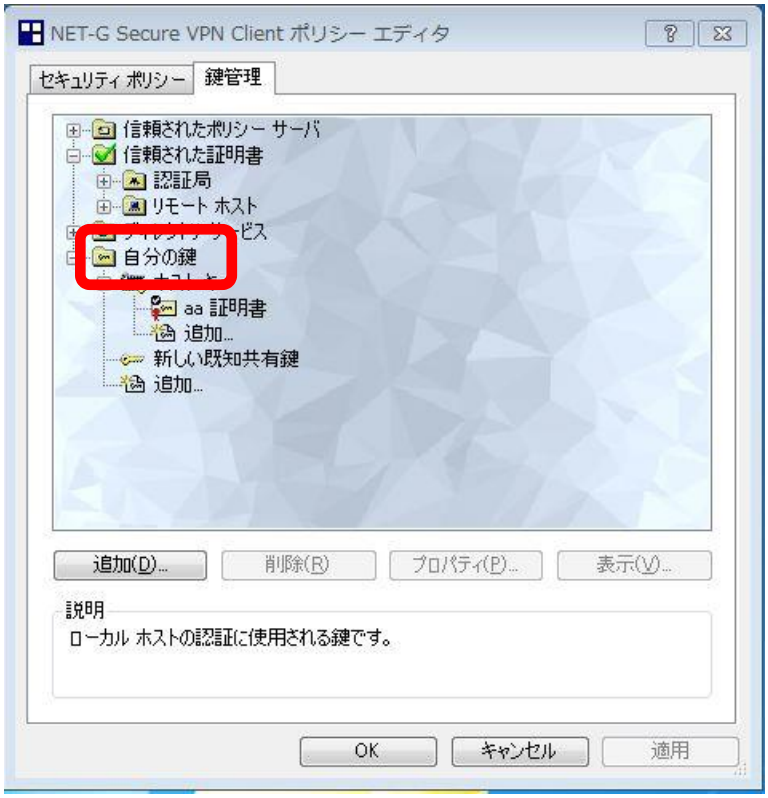
time zone 0900
タイムゾーンを設定します。通常はこのままで構いません。

consoleinfo autologout 8h
telnetinfo autologout 5m
シリアルコンソール、TELNETコネクションの入出力がない場合のコネクション切断時間を設定します。通常はこのままで構いません。

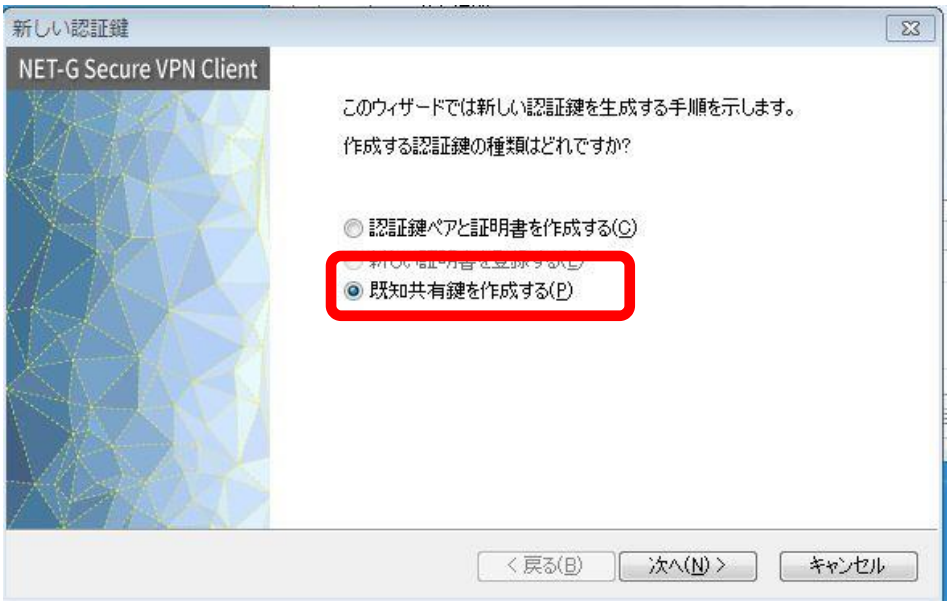
terminal charset SJIS
ターミナルで使用する漢字コードをShift JISコードに設定します。

NET-G1の設定例になります。NET-G2についても同様に設定を行ってください。
「ポリシーエディタを実行」を選択します。

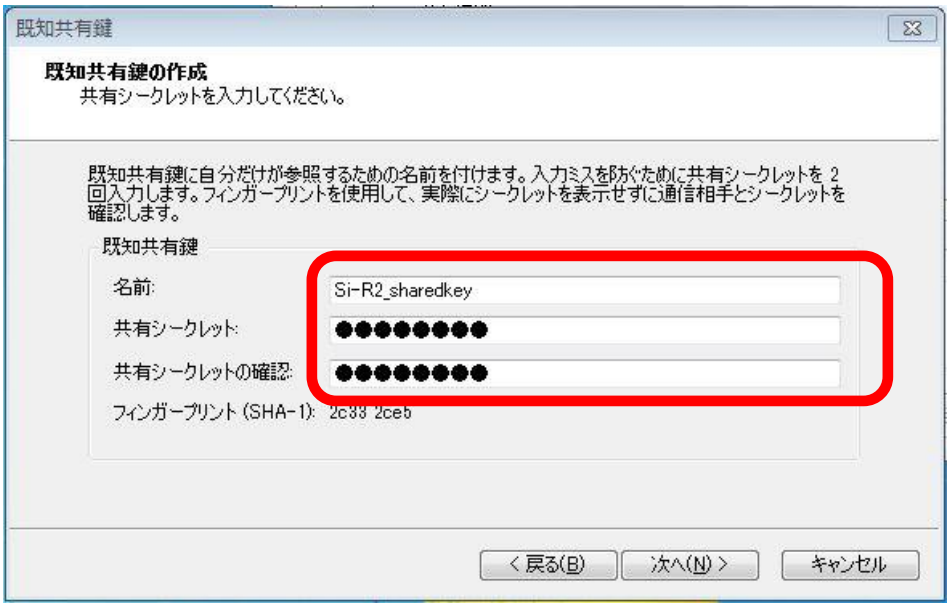
鍵管理タブの「自分の鍵」を選択した状態で右クリックし、「追加」を選択します。



「既知共有鍵を作成する」を選択し、次へをクリックします。

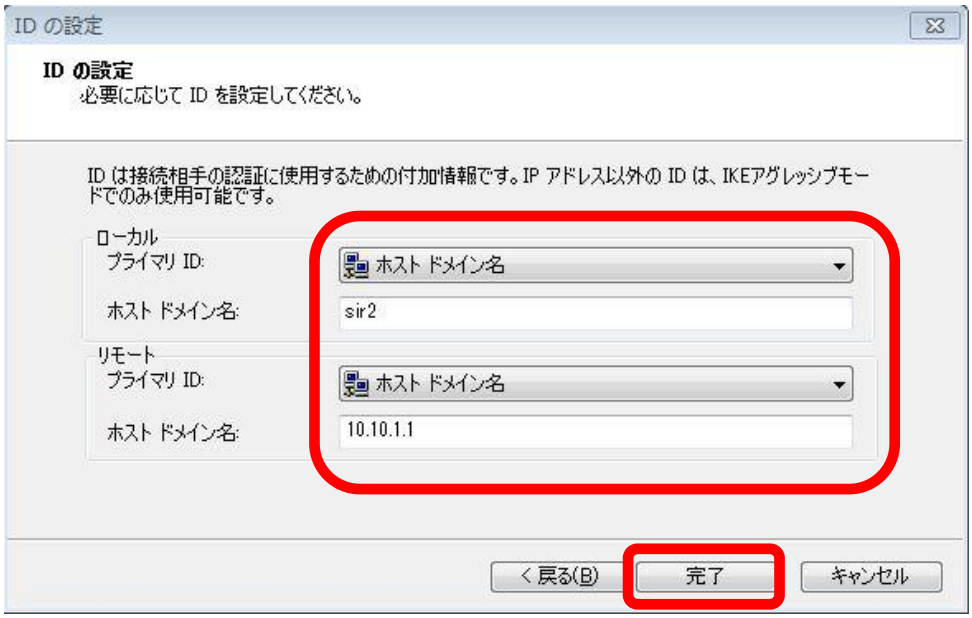


共有シークレットの設定を行います。今回の設定例では共有シークレットはsir2-keyと設定しています。この設定値はSi-R側のtemplate 0 ap 0 ike shared keyと一致している必要があります。名前はSi-R側の設定とは関係がないので任意の名前を設定してください。

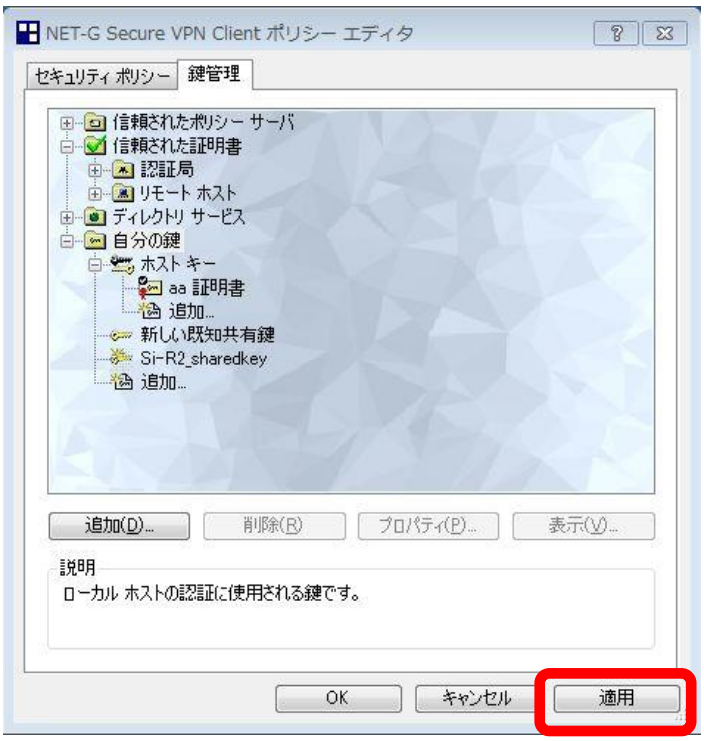


IDの設定を行います。ローカルIDおよびリモートIDを下のように設定してください。

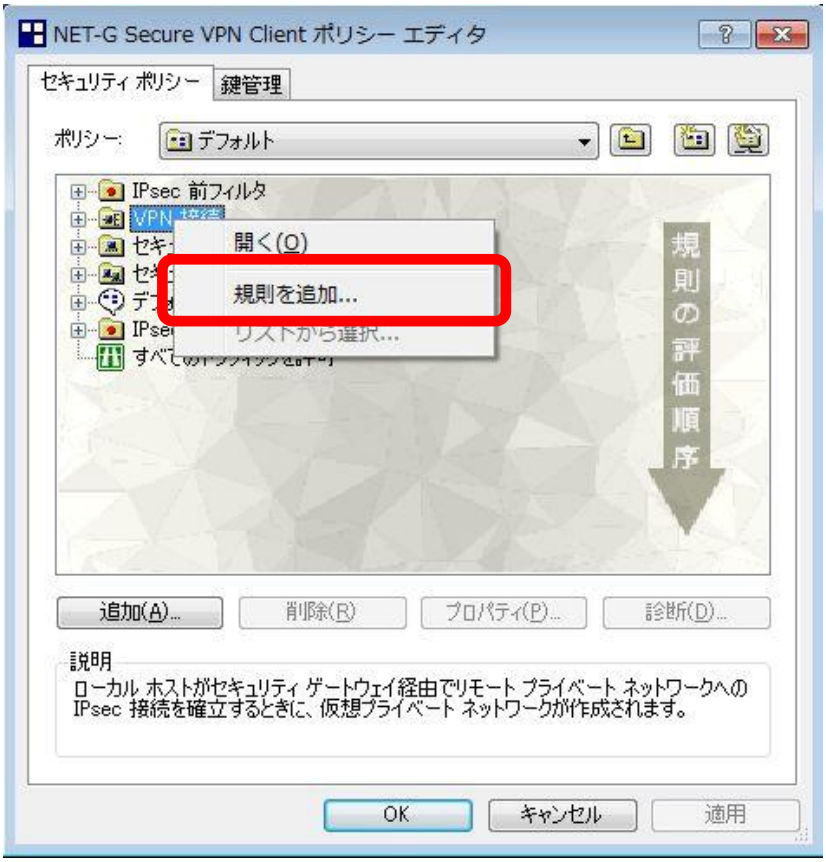
ローカルのホストドメイン名"sir2"はSi-R側のtemplate 0 ap 0 ike name remoteと一致している必要があります。リモートのホストIPアドレス"10.10.1.1"はSi-R側のtemplate 0 ap 0 tunnel localと一致している必要があります。設定が終了したら「完了」をクリックします。



「適用」をクリックします。

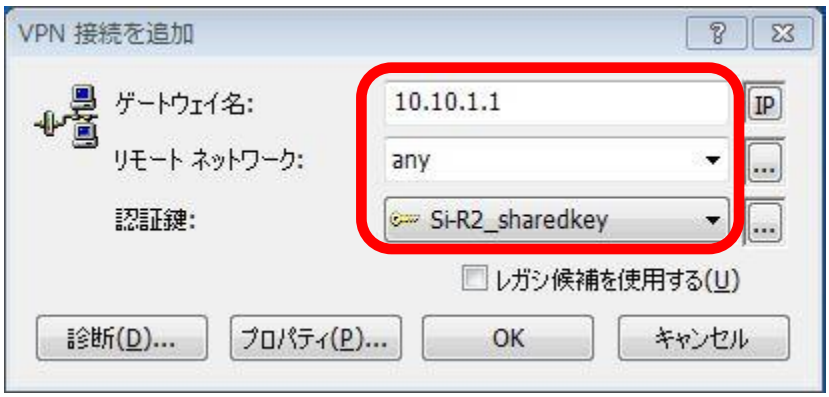


セキュリティーポリシータブの「VPN接続」を右クリックし、「規則を追加」を選択します。

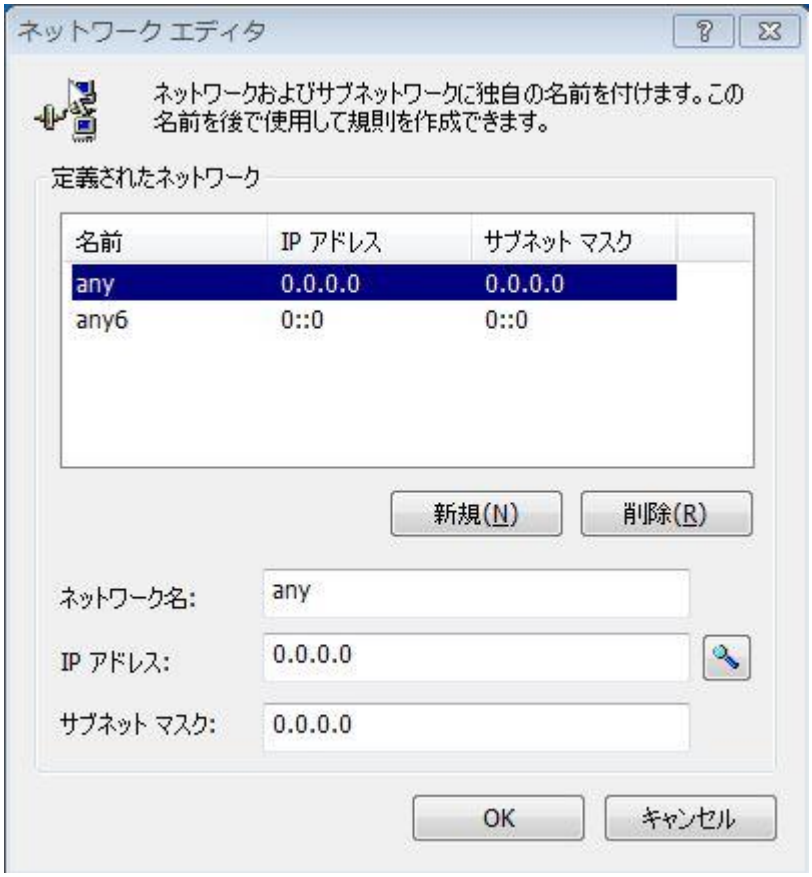


ゲートウェイ名、リモートネットワーク、認証鍵の設定を行います。

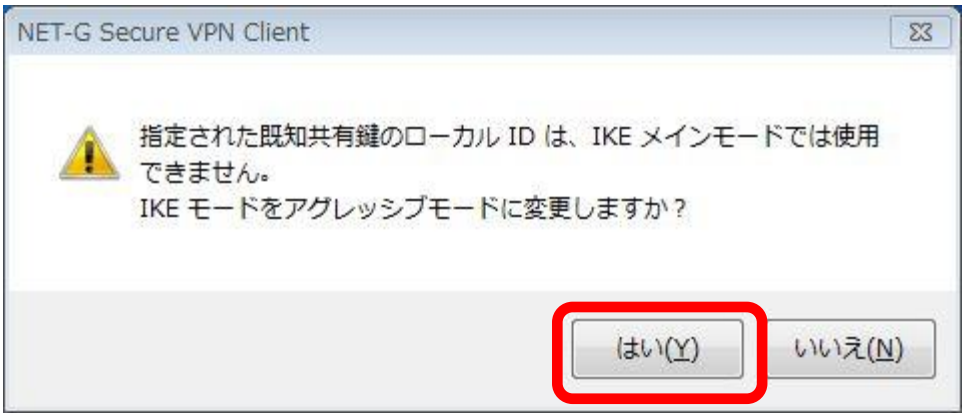
ゲートウェイのIPアドレス”10.10.1.1”はSi-R側のtemplate 0 ap 0 tunnel localと一致している必要があります。リモートネットワーク”any”はSi-R側のtemplate 0 ap 0 ipsec ike rangeの送信元ネットワークと一致している必要があります（Si-Rの設定はany4となっており、ここで設定しているanyと同等です）。認証鍵の設定は先ほど共有シークレットで設定した任意の名前をプルダウンメニューから選択します。



※なお、リモートネットワークをany以外に設定したい場合は、リモートネットワークのプルダウンメニュー右の"・・・"
ボタンをクリックすることで下記の画面となりここで設定が可能です。

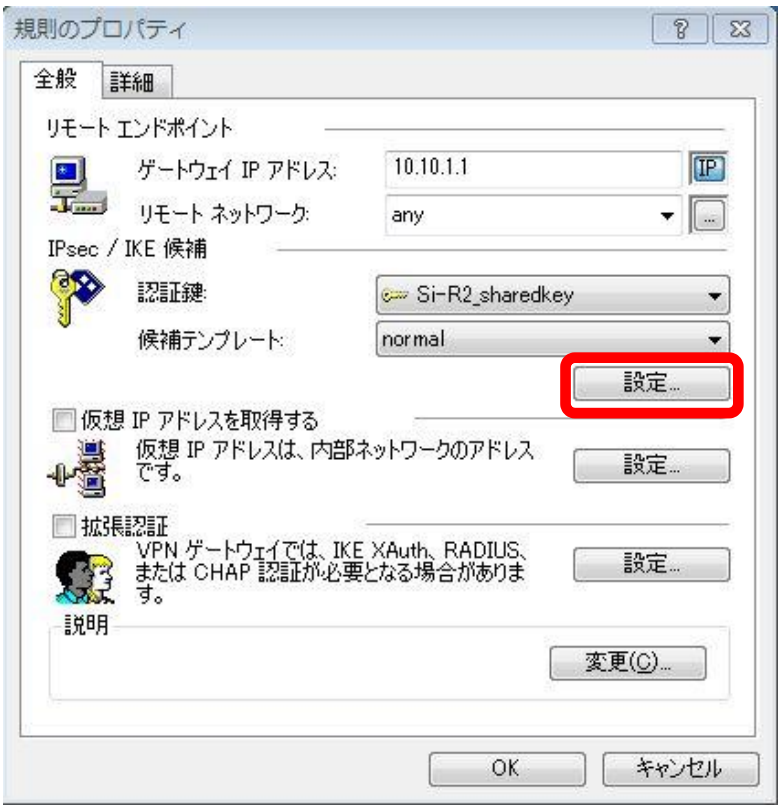


下記のメッセージが表示された場合は、「はい」をクリックします。

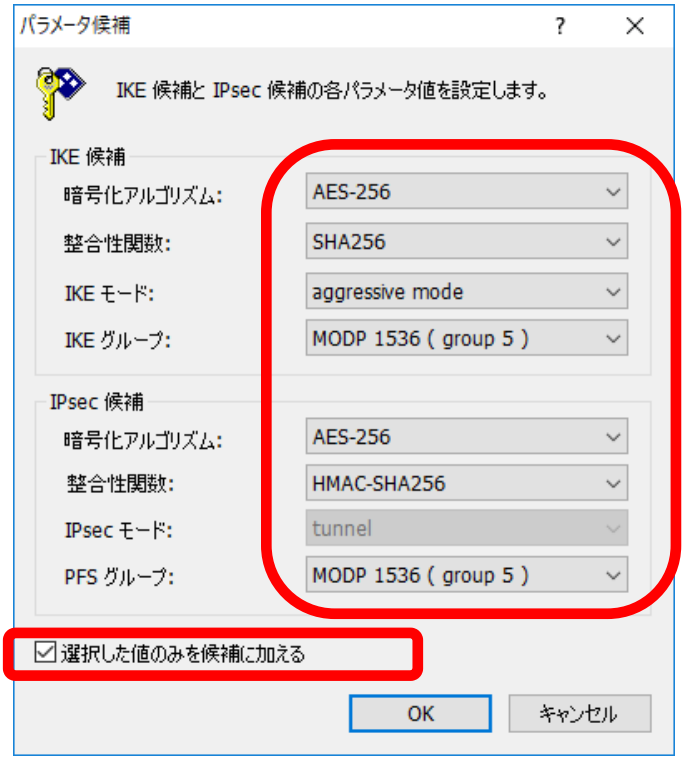


セキュリティポリシータブの「10.10.1.1 (any)」を選択し、「プロパティ」をクリックします。

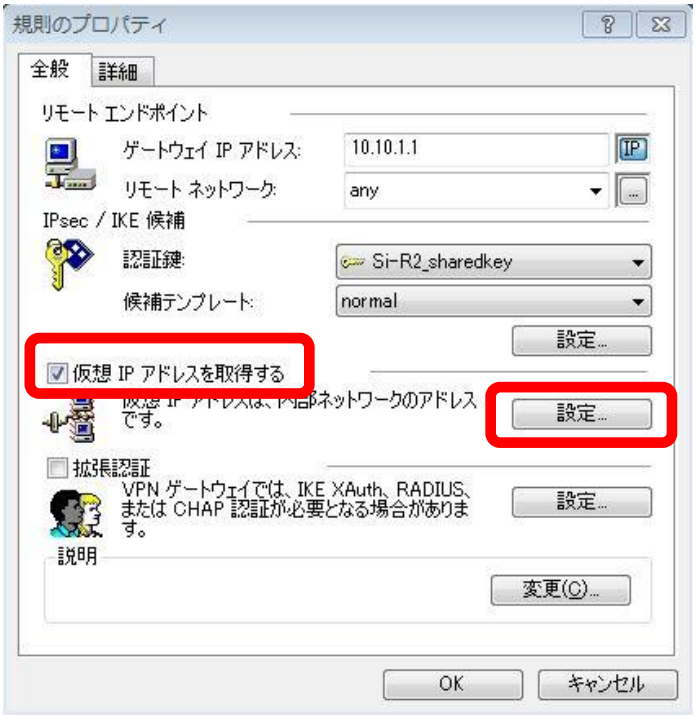
規則のプロパティ全般タブの一番上にある「設定」をクリックします。



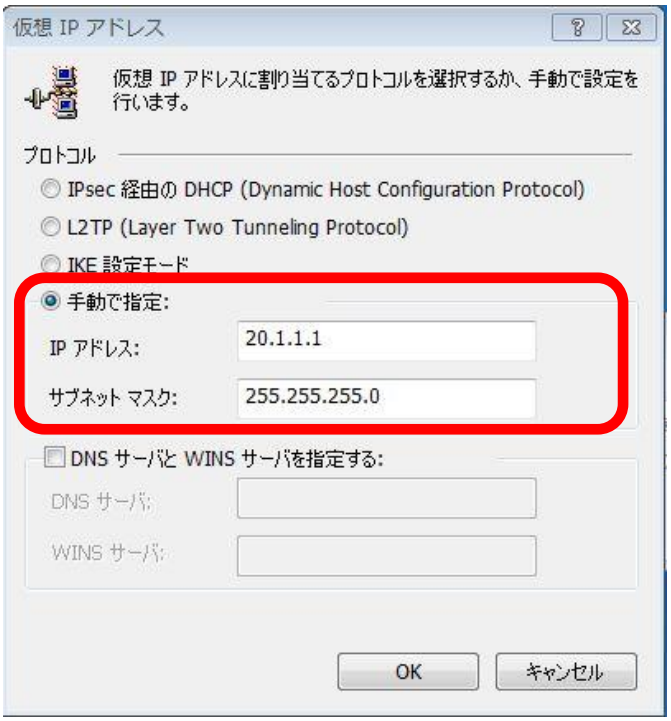
IKE（フェーズ1）とIPsec（フェーズ2）の各パラメタを設定します。Si-R側の各設定と一致させる必要があります。「選択した値のみを候補に加える」にチェックをつけます。チェックを忘れた場合、正常にIPsecが張れない可能性があるので必ずチェックを付けてください。



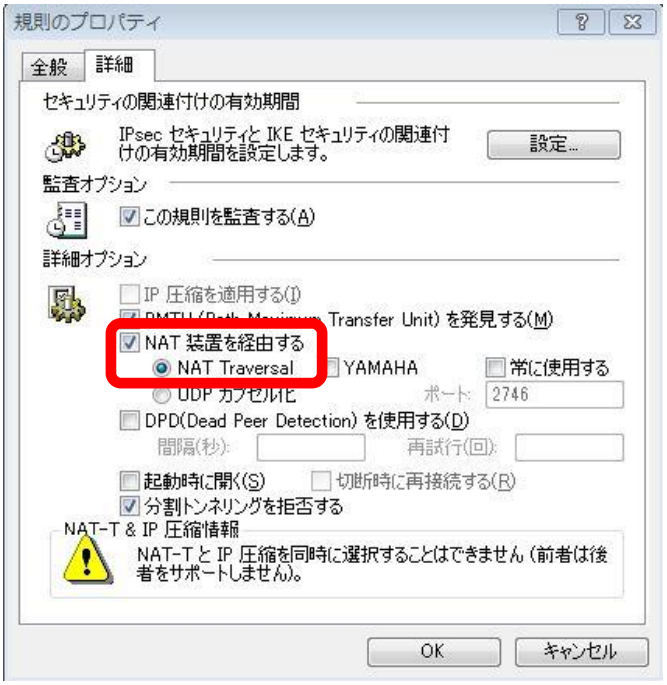
規則のプロパティ全般タブの中央にある、「仮想IPアドレスを取得する」にチェックをつけ、その右にある「設定」をクリックします。



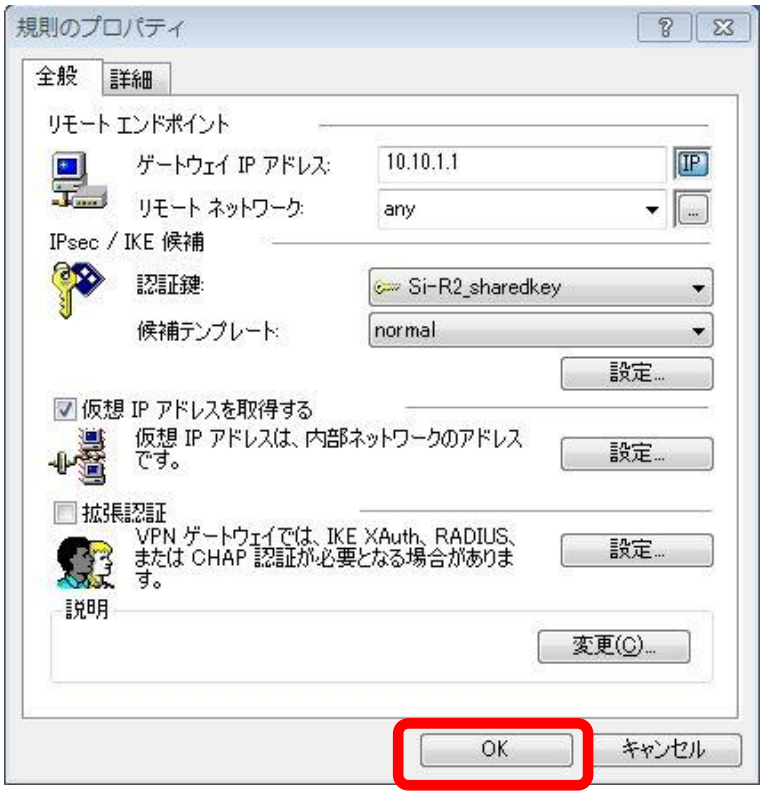
仮想IPアドレスの設定を行います。仮想IPアドレスとはプライベートネットワークへアクセスする際にこの端末が仮想的に利用するIPアドレスとなります。
「手動で指定」を選択し、IPアドレスとサブネットマスクを設定してください。ここで設定した、”20.1.1.1”はSi-R側のtemplate 0 ip route 0と一致している必要があります。



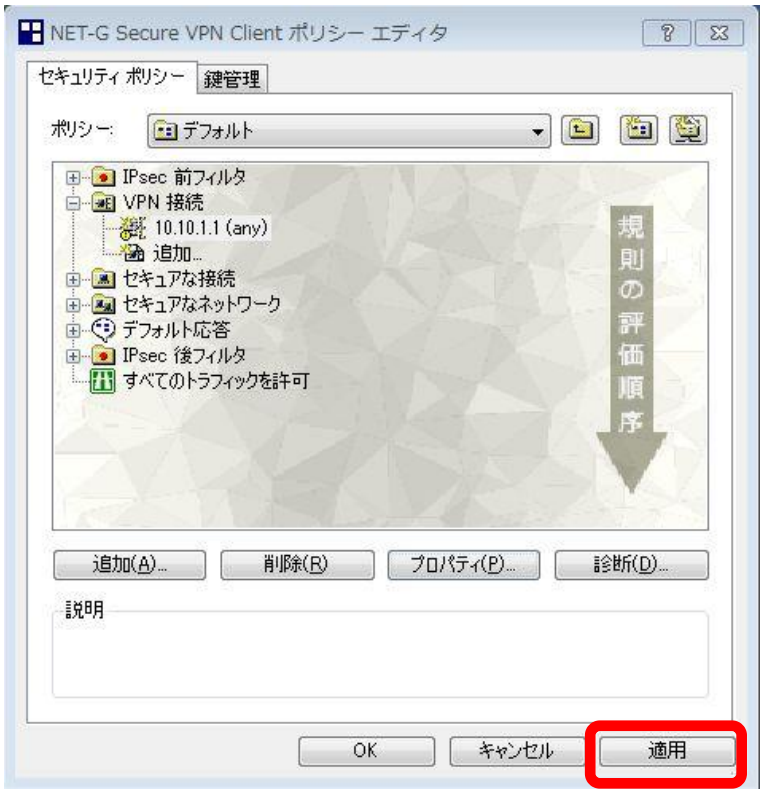
規則のプロパティ詳細タブの「NAT装置を経由する」にチェックをつけます。NAT Traversalを選択します。



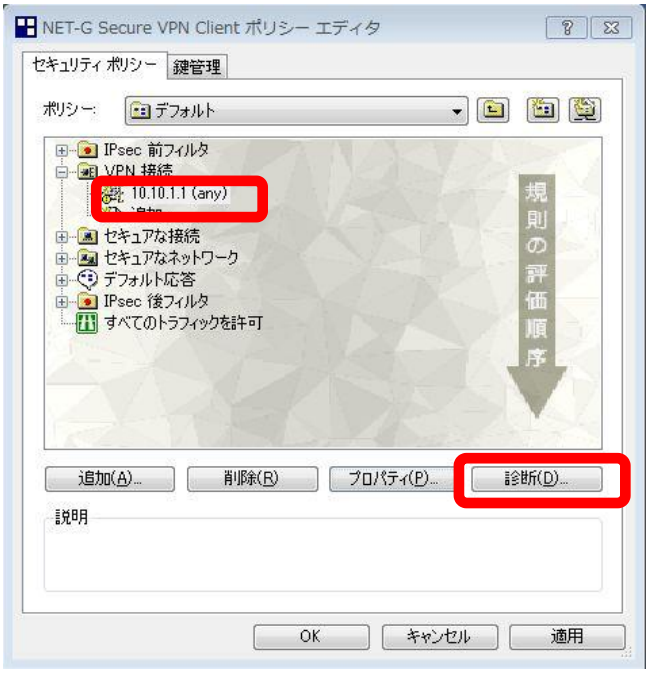
設定が終了したら、規則のプロパティで「OK」をクリックします。



「適用」をクリックします。設定は完了です。



診断を行うことで、NET-G、およびSi-R側の設定が正しいかを確認可能です。
セキュリティポリシータブで先ほど作成した10.10.1.1 (any)を選択し、診断をクリックします。



設定に問題が無ければ以下の結果が表示され、IKE SAとIPsec SAが正常に確立されていることが確認できます。